Ministerio de Agricultura y Ganadería

Servicio Nacional de Salud Animal

POLITICAS Y NORMAS GENERALES DE TECNOLOGIA DE INFORMACION

Departamento de Tecnología de Información

Contenido

Presentación

Marco Jurídico

La Contraloría General de la República ha emitido leyes y normativas para el control y administración en materia de tecnologías de información y comunicación, así como la Ley General de Control Interno y otras normativas relacionadas sobre este tema.

En el año 2007 el ente contralor emite las “Normas técnicas para la gestión y el control de las tecnologías de información” las cuales fueron publicadas en el Diario Oficial La Gaceta No 119 del Jueves 21 de junio de ese mismo año y en su Capítulo I, Artículo 1.1 se establece la necesidad que en cada Institución exista un marco estratégico de Tecnologías de Información, constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido.

Por lo tanto, en todas las instituciones del Estado deben existir manuales de políticas internas relativas a la administración de Tecnologías de Información. Para su cumplimiento, se definen en este documento las políticas que en esta materia, deben aplicarse para el Servicio Nacional de Salud Animal del Ministerio de Agricultura y Ganadería.

Ámbito de aplicación

Las políticas definidas en este documento son de aplicación para todo el Servicio Nacional de Salud Animal (SENASA), incluyendo las Direcciones Nacionales, Regionales, Programas y todas las organizaciones adscritas al SENASA, cuyas actividades se apoyan en instrumentos informáticos.

Actualizaciones de este manual

Este instrumento rige una vez que el jerarca institucional lo apruebe y haya ordenado su puesta en marcha de manera oficial.

Deberá ser revisado y actualizado formalmente por lo menos una vez cada año, siendo responsabilidad de la jefatura del Departamento de Tecnología de Información, en adelante denominado Departamento de TI, realizar este proceso.

Durante el proceso de implementación cualquier usuario podrá hacer observaciones, con el objetivo de mejorar y/o modificar cláusulas o políticas, las cuales se harán llegar a la jefatura del Departamento de TI.

Objetivos

Objetivo General

Mantener la confiabilidad, disponibilidad e integridad de la información, así como facilitar el mejor aprovechamiento de los recursos informáticos y las telecomunicaciones, que son propiedad o se encuentran a disposición del Servicio Nacional de Salud Animal, para alcanzar la misión institucional.

Objetivos Específicos:

- Utilizar los recursos tecnológicos de información y comunicación en forma responsable y apropiada, de conformidad con las disposiciones dadas en este manual y otras de carácter institucional, legal o emitido por otros órganos del Estado Costarricense, que guarden relación con normativas aplicables a la materia.
- Minimizar las interrupciones de los servicios asociadas a los sistemas informáticos y comunicaciones, ocasionados por uso inapropiado o por daños causados en forma accidental o intencional.
- Ordenar el desarrollo y mantenimiento de aplicaciones acordes con un modelo integral de información institucional e interinstitucional, para la colaboración de información de gran utilidad para la institución.
- Adquirir tecnología acorde a las necesidades institucionales aprovechando al máximo las capacidades de los funcionarios y el presupuesto asignado para esta materia.

Supervisión de las políticas

La supervisión del cumplimiento de las “Políticas Generales sobre Tecnologías de Información”, queda a cargo del Departamento de TI; razón por la cual está facultada para verificar en cualquier momento el cumplimiento de estas políticas y de las normativas vigentes en materias de tecnologías de información y comunicación.

Violación a las políticas

La infracción o incumplimiento de las políticas sobre tecnologías de información y comunicación, será notificado a la Dirección correspondiente a fin de que ésta proceda según corresponda. Durante el proceso de implementación se estará revisando el tema de cumplimiento y sanción con el Departamento de Recursos Humanos.

Este documento se estará revisando y/o actualizando por parte del Departamento de Tecnología de Información, con la finalidad de estarlo mejorando. Estas modificaciones serán aprobadas y comunicadas a través de la Dirección General.

Políticas para los servicios de tecnologías de información y comunicación

1. Políticas Generales

1. El Departamento de TI, será una unidad administrativa funcionalmente independiente, que le permitirá la ejecución de procesos de planeación, coordinación, ejecución y supervisión estratégica de los proyectos e inversiones de tecnología de información a nivel institucional. Para ello tendrá una dependencia jerárquica adecuada a este propósito, asociada directamente a la Dirección General de la institución.
2. Las políticas de tecnologías de información serán aprobadas por el jerarca del SENASA y divulgadas adecuadamente a través de los directores nacionales, regionales y sitio web institucional. Estas políticas serán materia obligada en los procesos de inducción a los nuevos funcionarios.
3. Todos los usuarios del SENASA, deberán conocer los documentos de Políticas relativos a Tecnología de Información y regirse en su actuar por los principios consignados en ellos
4. El Departamento de TI será responsable por la definición y ejecución de los presupuestos que el SENASA asigne en materia de tecnología de información. Estos presupuestos incluyente tanto presupuesto ordinario, extraordinario, donaciones o proyectos de cooperación, entre otros.
5. La jefatura del Departamento de TI tendrá la responsabilidad de ejercer la Secretaría de la Comisión Gerencial de Tecnología de Información.
6. La Dirección Administrativa y Financiera, las Direcciones Nacionales y Regionales brindarán el apoyo logístico, material, presupuestario y los recursos humanos necesarios al Departamento de TI, para que pueda cumplir adecuadamente sus funciones.
7. La Administración del SENASA procurará recursos suficientes en los presupuestos ordinarios, extraordinarios o de proyectos de cooperación; para satisfacer los requerimientos que se deriven de la puesta en ejecución de implementación de sistemas digitales para SENASA.

1. Concienciar a todos los funcionarios del SENASA, sobre su obligación de conocer y aplicar la normativa en materia de seguridad de TI para lograr un cambio favorable en la cultura organizacional.

2. Políticas Administrativas

2.1. Políticas para el planeamiento y administración de actividades

1. El Departamento de TI contará con un Plan Anual Estratégico con el cual se orientarán las actividades.

2. En los proyectos relacionados con desarrollo de aplicaciones, deberá aplicarse una metodología formal basada en los enfoques de ciclo de vida de sistemas y orientación a objetos mediante proceso unificado, para asegurar la adecuada administración y desarrollo.

2.2. Políticas sobre los servicios que ofrece el Departamento de TI

1. El Departamento de TI creará un registro de los servicios que ofrece a las dependencias del SENASA y los informará a través de la web.
2. Los servicios ofrecidos por el Departamento de TI, se solicitarán formalmente y siguiendo los procedimientos que se emitan para ese fin.

2.3. Políticas para el acceso físico al Departamento de TI y Áreas de TI

1. En general las oficinas de las Áreas de Tecnologías de Información son de acceso restringido, dadas las características del trabajo que se desarrolla en sus instalaciones.
2. Los funcionarios de las diferentes dependencias podrán ingresar a la recepción del Departamento TI, para efectos de solicitar servicios o consultas. Asimismo, podrán ingresar al interno de las oficinas siempre que haya un funcionario de TI que los atienda personalmente, manteniendo visibles sus correspondientes gafetes de identificación.

2.4. Políticas para la documentación y mantenimiento de manuales del Departamento de TI

1. Será política del Departamento de TI, documentar formalmente todas las actividades que realice en el desarrollo de los servicios que brinda a la Institución.
2. El Departamento de TI mantendrá un archivo de gestión de documentos, debidamente ordenado y clasificado para el registro y custodia de la documentación administrativa, correspondencia y de actividades técnicas que desarrolla. Mantendrá, como mínimo, dentro de sus archivos de gestión, las siguientes documentaciones:
    - Correspondencia interna mantenida con todas las dependencias del Ministerio
    - Correspondencia con entidades externas
    - Documentación de planeamiento estratégico de Tecnologías de Información
    - Documentación de planes anuales operativos
    - Documentación sobre solicitudes de servicio recibidas
    - Documentación de inventario de equipos de cómputo, periféricos y de telecomunicaciones
    - Documentación de inventario de software instalado en equipos
    - Documentación del mantenimiento correctivo de equipos de cómputo, periféricos y telecomunicaciones

- Documentación de licencias de software adquiridas
- Documentación de proyectos formalmente desarrollados
- Documentación administrativa de los funcionarios del Departamento

3. El Departamento de TI mantendrá en su archivo de gestión un Compendio de Manuales que contendrá como mínimo:
    - Manual de Políticas y Normas General Tecnologías de Información
    - Manual de Políticas de Uso de Equipo de Computo
    - Manual de Políticas de Correo Electrónico e Internet
    - Manual de Puestos del Departamento de TI
    - Manual de Procedimientos del Departamento de TI
4. El Departamento de TI utilizará toda la documentación formal definida en la organización para el desarrollo de trámites administrativos.

2.5. Políticas para la adquisición de nuevas tecnologías

1. Todos los procesos institucionales de adquisición de recursos informáticos, deben ser valorados y aprobados previamente por el Departamento de TI.
2. Para la adquisición de nuevos recursos de hardware, software y otros dispositivos tecnológicos, será política del Departamento de TI recomendar aquellos que ofrezcan calidad comprobada y sean referentes en el mercado nacional.
3. Para el trámite de adquisición de nuevos recursos informáticos, el Departamento de TI asesorará y apoyará a la Proveeduría Institucional, en la definición de las características tecnológicas y evaluación de ofertas mediante recomendaciones técnicas.
4. Para la adquisición de nuevos recursos, el Departamento de TI se fundamentará en los reglamentos y normativas de compras definidos para la Institución o proyecto de cooperación según sea el caso.
5. El Departamento de TI y la Proveeduría Institucional velará porque los recursos informáticos adquiridos sean enviados y utilizados por la misma Dirección en que surgió la necesidad de compra.

2.6. Políticas sobre inventario de equipo

1. El Departamento de TI mantendrá un inventario de equipo con las características de cada uno de ellos, tanto de la sede central como de las direcciones regionales, nacionales, oficinas cantonales y puestos fronterizos según corresponda.
2. El Departamento de TI colocará un mecanismo de seguridad en los equipos, los cuales estarán enumerados para el correspondiente control. La finalidad de estos mecanismos es controlar la integridad de los equipos que están bajo responsabilidad de los usuarios. En las Direcciones Regionales se contará con el apoyo del enlace de TI (donde exista y se haya

nombrado oficialmente), quien tendrá el control y la responsabilidad de la ubicación de los equipos. Para ello se gestionará con la Dirección Administrativa la adquisición de los mecanismos de seguridad durante el proceso de implementación continuo.

3. El mecanismo de seguridad no se podrá ser removido por nadie, excepto por los técnicos del Departamento de TI o el Personal de Apoyo Regional previamente autorizado, quienes rendirán un informe escrito de los cambios que sufriera el equipo y de las vulneraciones de los mecanismos.
4. El Departamento de TI deberá revisar el inventario del equipo por lo menos una veces al año, realizando los cambios que sean necesarios. Hará un informe a la Administración sobre las diferencias y/o deficiencias encontradas.

2.7. Políticas sobre reparación de equipos

1. Todos los usuarios deben acatar el procedimiento que el Departamento de TI implemente para controlar los servicios de reparación y la calidad de los mismos.
2. La obtención de fondos presupuestarios para la adquisición de repuestos y accesorios será gestionada a través del Departamento de TI, quedando condicionado a la factibilidad técnica y presupuestaria.
3. El Departamento de TI tendrá un control de las garantías de los equipos adquiridos para hacer cumplir los compromisos contractuales. Los equipos no cubiertos procederán a ser reparados en el sitio mismo o en el taller. Podrá además ser enviado a talleres externos especializados y el costo será gestionada a través del Departamento de TI, quedando también condicionado a la factibilidad técnica y presupuestaria.

3. Políticas relativas a sistemas de Información

3.1. Políticas generales para el desarrollo de sistemas de información

1. En general para el desarrollo de sistemas “in house” o “outsourcing”, “todas las Direcciones del SENASA, deben armonizar sus procedimientos de captura y registro de información referente a Establecimientos y Actividades Agropecuarias, de acuerdo con el marco conceptual y el modelo de clasificación que se define para el actual Sistema Integrado de Registro de Establecimientos Agropecuarios (SIREA).
2. El Departamento de TI desarrollará y dará mantenimiento a los sistemas de información que la organización requiera, de acuerdo a los recursos humanos y tecnológicos que tenga a su disposición para este fin.

3.2. Políticas para el desarrollo interno de sistemas de información

1. El desarrollo de aplicaciones o sistemas se hará bajo el concepto de tecnología web.
2. El desarrollo de sistemas de información se hará mediante proyectos debidamente formalizados, administrados y de acuerdo con la metodología y estándares del Departamento de TI, los cuales estarán establecidos en su respectivo manual de Desarrollo de Sistemas.
3. Las solicitudes de nuevos sistemas de información a desarrollar, deberán ser formalmente presentadas por las Jefaturas, con el formato y los requerimientos que el Departamento de TI defina.
4. Las solicitudes de nuevos sistemas de información, solicitadas por las diferentes dependencias del Ministerio, serán evaluadas y aprobadas por el Departamento de TI de acuerdo con las prioridades que se determinen.
5. El proceso de desarrollo de sistemas debe contemplar las etapas de determinación de requerimientos, análisis del sistema, diseño del sistema, desarrollo de la programación, implementación, pruebas, puesta en producción.

3.3. Políticas para el desarrollo externo ("outsourcing") de sistemas de información

1. El Departamento de TI podrá recurrir al desarrollo sistemas de información por "outsourcing", cuando no cuente con el recurso humano y/o tecnológico necesario, para llevar a cabo los desarrollos de forma interna, además cuando otros factores como el tiempo no lo permitan.
2. Las solicitudes de nuevos sistemas de información a desarrollar en la modalidad de "outsourcing", deberán ser formalmente presentadas por las Jefaturas, en forma escrita e indicando en éstas los requerimientos generales por cubrir.
3. Para los proyectos de desarrollo de sistemas de información por "outsourcing", deberá establecerse un contrato formal entre el SENASA y la empresa proveedora del servicio, en donde se definan las condiciones de la contratación, las tecnologías a utilizar y los mecanismos de control.
4. El control y monitoreo del avance de proyectos de sistemas de información por "outsourcing" estará a cargo del Departamento de TI.
5. Para el desarrollo de proyectos de sistemas de información por "outsourcing", deberán existir dos o más funcionarios que cumplan las funciones de "contraparte" de la Institución, quienes deberán ser profesionales del Departamento de TI y del área usuaria.
6. El Departamento de TI estará pendiente que las empresas contratadas para el desarrollo de sistemas de información, brinden la capacitación a sus funcionarios en administración, uso y mantenimiento del nuevo sistema de información.

7. Los sistemas de información desarrollados por empresas externas, deberán ser entregados por éstas, de manera formal y debidamente documentados, incluyendo los entregables de documentación definidos por el Departamento de TI.
8. Los programas desarrollados o adquiridos externamente serán de uso exclusivo del SENASA, y no se permite el uso para funciones que no correspondan a las operaciones normales del SENASA, excepto que exista algún convenio de cooperación entre instituciones.

3.4. Políticas sobre mantenimiento de sistemas de información

1. Será considerado como mantenimiento de sistemas de información todas las acciones que impliquen modificaciones, correcciones, mejoras o adiciones a los sistemas de información, que soliciten los usuarios de cualquier dependencia del SENASA.
2. El personal del Departamento de TI será el encargado de dar el mantenimiento ordinario a los sistemas de información que se desarrollen en o para el SENASA.
3. El Departamento de TI definirá el procedimiento y las formalidades necesarias que orienten la forma en que serán desarrolladas las actividades de mantenimiento de sistemas de información.
4. En caso de requerirse mantenimiento de sistemas de información tipo “outsourcing”, se aplica las mismas políticas anteriores “Políticas para el desarrollo externo (“outsourcing”) de sistemas de información”.

4. Políticas relativas a bases de datos.

4.1. Políticas para la creación de bases de datos

1. El Departamento de TI será el encargado de diseñar física y lógicamente las bases de datos, que utilizarán los sistemas de información que se desarrollen internamente.
2. El Departamento de TI permitirá la creación de bases de datos a empresas contratadas para este fin o para el desarrollo de sistemas de información, siempre que se desarrollen según los estándares definidos en el respectivo Manual de Bases de Datos, y que entreguen la documentación técnica especificada en dicho manual.
3. En la creación de nuevas bases de datos se deberá generar la documentación necesaria y suficiente, que permita comprender su estructura física y lógica, así como su contenido.
4. En la definición de nomenclatura para las bases de datos, debe respetarse el Manual de Estándares correspondiente elaborado por el Departamento de TI.

5. El Departamento de TI hará uso de una herramienta para el modelaje de datos, creación y generación de base de datos, para lo cual debe adquirirse la respectiva licencia y la capacitación para su manejo.

4.2. Políticas para la migración de información de bases de datos

1. Toda migración de base de datos deberá ser realizada por personal técnico capacitado interno o personal externo, el cual deberá ser supervisado por un profesional del Departamento de TI.
2. Antes de cualquier proceso de migración se deberán realizar los respaldos respectivos, así como realizar previamente una prueba de la migración en un servidor de pruebas, para garantizar que el proceso de migración funciona correctamente.
3. En las actividades de migración de información a bases de datos, se deberá seguir el procedimiento definido por el Departamento de TI para evitar atrasos y complicaciones, así como dejar documentado en una bitácora todo lo realizado para futuras migraciones.

4.3. Políticas sobre instalación de bases de datos

1. Toda instalación de base de datos deberá ser realizada por el personal técnico capacitado del Departamento de TI, o en su defecto por personal de empresas contratadas para estos efectos, bajo la supervisión del Departamento de TI.
2. Antes de cualquier instalación deberán realizarse los respaldos respectivos para evitar accidentes y garantizar la recuperación de la base de datos.
3. Para la instalación de bases de datos se deberá seguir el procedimiento definido por el Departamento de TI para prevenir que se den atrasos o complicaciones, así como dejar documentado en una bitácora todo lo realizado.

4.4. Políticas sobre administración y mantenimiento de bases de datos

1. Todo mantenimiento a las bases de datos deberá ser realizado por personal técnico capacitado interno o externo, quienes deberán ser supervisados por el profesional responsable de esa tarea del Departamento de TI.
2. Antes de cualquier proceso de mantenimiento a la base de datos, se deberán realizar los respaldos respectivos para estar prevenidos contra cualquier accidente que se pudiera presentar.
3. Todo cambio o ajuste hecho en el proceso de mantenimiento, se deberá dejar documentado en una bitácora para efectos de control y seguimiento.

4.5. Políticas de tiempos de almacenamiento de información en bases de datos

1. El Departamento de TI deberá garantizar la conservación permanente de toda la información almacenada en las bases de datos de los servidores, que esté directa o indirectamente relacionada con las actividades del SENASA.
2. La información deberá ser conservada durante el período que se defina en la tabla de plazos de conservación, labor en la cual tendrá concurso el Archivo Central de la Institución.
3. Todo acceso a las bases de datos del SENASA deberá contar con los mecanismos adecuados y controlados, que garanticen su seguridad, su integridad y la confidencialidad de la información almacenada.
4. Toda transacción que se ejecute en las bases de datos, dejará las pistas adecuadas de auditoría, para poder ejercer un control adecuado, de todas las modificaciones que se hagan en éstas mediante el uso de bitácoras.
5. Deberán de mantenerse y aplicarse sistemas de respaldos para todas las bases de datos del SENASA, con el fin de garantizar su conservación.
6. Deberán existir planes de recuperación de la información de las bases de datos, para garantizar la continuidad del servicio que se presta por medio de los sistemas de información.

4.6. Políticas de seguridad en bases de datos

1. Todo acceso a las bases de datos del SENASA deberá contar con los mecanismos adecuados y controlados, que garanticen su seguridad, su integridad y la confidencialidad de la información almacenada.
2. Toda transacción que se ejecute en las bases de datos, dejará las pistas adecuadas de auditoría, para poder ejercer un control adecuado, de todas las modificaciones que se hagan en éstas mediante el uso de bitácoras.
3. Deberán de mantenerse y aplicarse sistemas de respaldos para todas las bases de datos del SENASA, con el fin de garantizar su conservación.

5. Políticas relativas a redes y telecomunicaciones

5.1. Políticas para el uso de las redes de datos

1. El Departamento de TI será la dependencia responsable de la administración y uso de la red interna de datos.

2. El Departamento de TI garantizará el acceso controlado en la red interna de datos a los funcionarios del SENASA que así lo requieran.
3. Los usuarios accederán a la red de datos por medio de un código de acceso que les asignará el administrador de la red.
4. El código de acceso a redes que se asigne será único y exclusivo para cada usuario, el cual será responsable por su uso.
5. Todas las operaciones que se efectúen por medio de las redes internas serán responsabilidad única del usuario al que se le asignó el código relacionado con las mismas.
6. El Departamento de TI monitoreará periódicamente los accesos a la red interna mediante herramientas de seguridad y administración.
7. No es permitido a ningún funcionario, excepto a los técnicos de redes, manipular los componentes activos de la red (switches, routers, dispositivos inalámbricos, cableado, etc.).
8. No se permitirá la instalación de puntos de acceso de redes inalámbricas con conexión a la red del SENASA sin la debida información y autorización del Departamento de TI. En caso de detección de un punto de acceso no autorizado se procederá a su inmediata desconexión de la red Institucional.
9. No está permitida la conexión de equipos con nombres o direcciones no registrados.
10. No se permite el empleo de mecanismos para la manipulación de direcciones de red o cualquier otro uso que pueda afectar a la topología o a la estructura lógica de la red.
11. El Departamento de TI solamente prestará apoyo a los equipos conectados a la red institucional; a estos efectos, se consideran conectados a la red del SENASA los equipos que accedan a la misma de forma remota a través de los medios proporcionados por el Departamento de TI.
12. Los equipos electrónicos de gestión e infraestructura de la red del SENASA serán instalados, configurados y mantenidos exclusivamente por el Departamento de TI.
13. Ningún usuario está autorizado a utilizar analizadores del tráfico que circula por la red del SENASA.Igualmente está prohibido utilizar herramientas de rastreo de puertos o que permitan detectar vulnerabilidades. El uso de estas herramientas sólo está permitido a los administradores de la red y bajo situaciones especiales (incidentes de seguridad, denuncias de usuarios, etc.) que lo justifiquen.
14. El Departamento de TI pondrá en funcionamiento herramientas de control que posibiliten detectar, analizar y bloquear accesos no permitidos, (aquellos que no guarden relación con aspectos de trabajo) que pongan en riesgo la seguridad de los recursos informáticos y atenten contra su desempeño.

6. Políticas relativas al servicio de Internet y correo electrónico

6.1. Políticas para el acceso a servicios de Internet y correo electrónico

1. Los servicios de Internet y correo electrónico serán administrados por el Departamento de TI.
2. Para la comunicación oficial del SENASA debe utilizarse la cuenta de correo institucional, en la medida de las posibilidades.
3. El acceso a los servicios de Internet y correo electrónico estarán disponibles para todos los usuarios del SENASA, si las condiciones de infraestructura tecnológica y administrativa lo permiten.
4. El correo electrónico institucional es una herramienta de comunicación e intercambio oficial de información y no una herramienta de difusión indiscriminada de información.
5. El uso de los servicios de Internet y correo electrónico deberá ser exclusivamente para apoyar y mejorar la calidad de las funciones administrativas y técnicas.
6. El Departamento de TI asignará las cuentas de correo de acuerdo a las licencias disponibles.
7. Está prohibido facilitar u ofrecer las cuentas de correo a terceras personas.
8. El servidor principal de correo electrónico debe mantener actualizada la herramienta de detección de virus para los correos entrantes y salientes.
9. Se prohíbe a los empleados formar parte de cadenas de mensajes o SPAM, ya que esto contribuye a la saturación de las redes de telecomunicación y facilita la divulgación de su cuenta de correo y la proliferación de virus en la red.
10. Se prohíbe a los funcionarios que tengan acceso al servicio de correo electrónico abrir mensajes de procedencia desconocida.
11. El funcionario que tenga acceso a servicios de correo electrónico debe evitar divulgar su cuenta a personas o entes desconocidos.
12. Ningún equipo que esté designado como servidor debe tener asociada una cuenta de correo electrónica.
13. Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar todos los lineamientos referentes al uso inapropiado del lenguaje.
14. Los funcionarios deben realizar revisiones periódicas de los mensajes almacenados con el fin de no mantener información innecesaria.
15. El Departamento de Recursos Humanos deberá notificar al Departamento de TI cuando se deba crear, cerrar o inhabilitar .
16. El usuario debe atender a los avisos de actualización automática del programa de detección de virus e informar al Departamento de TI, cuando la actualización no se realice satisfactoriamente.
17. Los valores de seguridad, de aceptación de cookies y los certificados de los navegadores o browser no deberán ser cambiados, excepto por indicaciones del Departamento de TI.
18. Para el envío de mensajes se aplicarán las siguientes reglas:

    a) Se utilizará siempre el campo de Asunto, a fin de resumir el tema del mensaje.

    b) No se enviarán mensajes a personas desconocidas, a menos que se trate de un asunto oficial que las involucre.

    c) No se enviarán mensajes a listas globales, a menos que el propietario sea la persona autorizada por el superior para enviar mensajes que involucren a toda la Institución.

e) La divulgación de mensajes de interés general (actividades internas, invitaciones, notas luctuosas, entre otros) deberá coordinarse con la Unidad de Comunicación y Notificación el cual definirá el procedimiento para tal fin.

19. Está prohibida la utilización abusiva del correo electrónico y de las listas de distribución incluyendo la realización de prácticas tales como:

- En caso de que fuera necesario un envío masivo se recomienda usar las listas de distribución o usar el campo de "copia oculta" (Bcc ó Cco) para poner la lista de destinatarios, o bien ponerse en contacto con el Departamento de TI.
- Actividades comerciales privadas.
- Propagación de cartas encadenadas o participación en esquemas piramidales o actividades similares.
- El insulto, la amenaza o la difamación a cualquier persona.
- Suscribirse a periódicos, revistas, semanarios, buscadores de parejas, chats; ni a ningún otro tipo de actividades o boletines electrónicos que no sea el estrictamente relacionado con el área profesional de trabajo del funcionario.
- Descargar archivos de música, programas, videos, pornografía y cualquier otro tipo de información que no guarde estricta relación con el área profesional del funcionario. El Departamento de TI procurará tomar las previsiones del caso para que se bloquee por medio de software especializado, el acceso no autorizado a los servicios antes mencionados.

7. Políticas relativas al hardware

7.1. Políticas de responsabilidad

1. El hardware que se encuentra en el área de servidores y los armarios de comunicaciones es responsabilidad directa del personal del Departamento de TI, que tendrá que velar por su uso y cuidado.
2. Los otros equipos de cómputo quedan bajo la responsabilidad del usuario al que se asignen. Estos tendrán la obligación de cuidarlos, mantenerlos limpios y velar por su buen funcionamiento. En el caso de existir algún problema con el equipo deberán de reportarlo inmediatamente al Departamento de TI para que se proceda a su revisión.
3. Los equipos portátiles (laptops, computadoras de Bolsillo, Agendas electrónicas, tablets, HandHeld, etc), serán asignadas a los usuarios con el objetivo de cumplir sus funciones y no deberán utilizarlo para uso personal.
4. Es responsabilidad del usuario custodiar los equipos portátiles asignados; por lo que deberá tomar las medidas de seguridad correspondiente dentro y fuera de la institución para evitar el robo del equipo o información. En caso de robo, deberá reportarlo inmediatamente a la Unidad de Bienes de la Dirección Administrativa Financiera y al

Departamento de TI, además de realizar la respectiva denuncia a la autoridad policial respectiva.

5. Queda entendido que los recursos informáticos asignados a cada usuario lo serán en calidad de herramienta de trabajo; como tal se encuentran permanentemente bajo dominio y control del SENASA, sin perjuicio del derecho a la privacidad de la información almacenada y demás derechos fundamentales establecidos por la Constitución Política.
6. Es responsabilidad del Departamento de TI hacer cumplir las garantías respectivas de cada uno de los equipos; para tal razón se deberán respetar los sellos de garantía que vienen adheridos a los equipos, y velar porque el usuario final no los despegue.
7. Es responsabilidad del Departamento de TI valorar la necesidad de sustituir algún equipo cuando ya éste no garantice la funcionalidad y operatividad adecuada.

7.2. Politicas de mantenimiento del hardware instalado

1. Los usuarios tienen el deber de informar sobre el rendimiento de cada equipo, para que sea valorado y de ser necesario mejorado.
2. Las ampliaciones, modificaciones o adquisición de equipo de cómputo, así como la actualización y compra de software, se harán únicamente por funcionarios del Departamento de TI.
3. La entrega, puesta en funcionamiento y cambio de equipo entre las diferentes dependencias del SENASA, se efectuará en coordinación con el Departamento de TI, utilizando para ello los procedimientos establecidos al efecto.
4. En el caso de fallas técnicas del equipo de cómputo, el Departamento de TI realizará un diagnóstico preliminar, con el objeto de procurar la solución, o en su defecto, girar las instrucciones del procedimiento a seguir para su reparación.
5. Los equipos de cómputo no podrán ser desmantelados, cambiados, abiertos ni reparados por los usuarios de las oficinas. Asimismo, sus componentes (entiéndase “mouse”, disco duro, teclado, memoria, fuente de poder, tarjeta madre, entre otros) no podrán ser removidos por personal no autorizado por el DTI, salvo aquellos casos específicos autorizados por el DTI para atención de fallas técnicas en equipos de cómputo de oficinas regionales.

7.3. Políticas de resguardo de Activos informativos

1. El Departamento de TI llevará y mantendrá el inventario de los recursos informáticos así como el control de la ubicación de los equipos de cómputo en las dependencias del

SENASA, así como de las licencias de uso del software adquirido. Igualmente cada Dirección o Unidad debe asignar un responsable de elaborar y mantener su inventario de recursos informáticos y deberá informar a su superior inmediato y al Departamento TI, sobre cualquier cambio del estado o ubicación del activo.

2. Los equipos de cómputo no podrán ser trasladados a otras oficinas que no sean del SENASA, salvo para alguna situación específica siempre que se cuente con la debida autorización de la Dirección General, lo cual se hará del conocimiento del Departamento de TI y a la Unidad de Bienes de la Dirección Administrativa Financiera.

7.4. Políticas para el desecho de equipos electrónicos

1. Los equipos electrónicos a ser desechados, será revisados por funcionarios del Departamento de TI, generando un acta de desecho la cual será entregada a la Unidad de Bienes como evidencia de su daño u obsolescencia para que proceda con el respetivo desecho.
2. El SENASA procurará la entrega de sus desechos tecnológicos a empresas recicladoras que cumplan con las normativas vigentes de protección al medio ambiente.

8. Políticas relativas al software

8.1. Políticas sobre el uso de licencias de software

1. Según Decreto Ejecutivo Nº 30151-J del 01 de febrero de 2002, en su Artículo 1 se indica: “Se ordena que todo el Gobierno Central se proponga diligentemente prevenir y combatir el uso ilegal de programas de cómputo, con el fin de cumplir con las disposiciones sobre derechos de autor que establece la Ley Nº 6683 y sus reformas…” Así las cosas, los programas que se utilizarán en los equipos del SENASA tendrán licencia, de lo contrario es ilegal y debe eliminarse de inmediato.
2. El Departamento de TI dará la asesoría necesaria a los funcionarios del SENASA en el tema de licencias. Los usuarios deben asegurarse que disponen de las licencias adecuadas al uso que hagan del respectivo software, ya sea mediante licencias adquiridas de forma centralizada por el SENASA (para software de uso común), por la adquisición individual de las correspondientes licencias, o bien por el uso de software libre. De no ser así, la responsabilidad recaerá totalmente sobre el usuario.
3. El Departamento de TI llevará un registro actualizado de los equipos y las licencias vigentes en el SENASA para informar a las respectivas instancias a este respecto.

4. Software propiedad del SENASA. Se prohíbe la instalación de software propiedad del SENASA en equipos que no pertenezcan a la institución. En los casos de convenios de cooperación debe existir una cláusula que así lo permita.
5. El Departamento de TI dará de baja todos los equipos que estén al margen de la ley, en lo que respecta al cumplimiento de la Ley de Derechos de Autor, lo cual se hará en un plazo razonable, que será comunicado al responsable de la dirección o departamento respectivo.
6. La Dirección Administrativa y Financiera gestionará mediante los presupuestos ordinarios y extraordinarios , la compra de licencias de "software" con la finalidad de que siempre el SENASA se mantenga al día con el uso de licencias. Esta función la hará mediante el concurso y petición del Departamento de TI.
7. El Departamento de TI removerá cualquier programa de las máquinas cuando no exista licencia, sin responsabilidad para ésta de los problemas que ocasione directa o indirectamente. Llevará un registro de los programas instalados ilegalmente, para que, ante la reincidencia de mantener programas instalados en forma ilegal, se proceda a reportar el asunto al Departamento de Recursos Humanos o ante las autoridades superiores, para aplicar la sanción que corresponda por desobediencia según el Reglamento Interno del MAG, lo cual debe tipificarse como falta grave. Para ello, el Departamento de TI cuidará de no violentar el derecho a la privacidad de las personas, solicitando previamente la autorización al usuario para proceder con la remoción del programa ilegal.
8. Los medios de instalación originales o acceso a los portales de descarga serán custodiados por el Departamento de TI.

8.2. Políticas para la instalación de Software

1. El Departamento de TI es la responsable de la instalación de los programas de software en cada una de las computadoras del SENASA.
2. Queda completamente prohibido que los usuarios realicen instalaciones de cualquier tipo de software en sus computadoras. De requerir un software específico debe solicitarse al Departamento de TI para que se valore la necesidad de su instalación.
3. Todo software que se instale en las computadoras del SENASA deberá contar con su respectiva licencia y su instalación deberá ser autorizada por la jefatura del Departamento de TI.
4. Queda prohibida la instalación del software adquirido por el SENASA en equipos que no sean de su propiedad.

5. El personal del Departamento de TI deberá mantener un inventario de software y programas instalados en cada una de las computadoras. Este inventario deberá revisarse y actualizarse una vez al año.
6. Para la administración y el manejo seguro de la información que se almacena en los computadores del SENASA y para evitar su utilización por personas no autorizadas, se utilizarán los sistemas operativos que ofrezcan mayor seguridad.
7. Conforme se adquieran nuevas versiones del Software el Departamento de Tecnología de Información realizara la respectiva instalación en los equipos de la institución.
8. El software que debe residir en el disco duro de cada computadora y ser utilizado por los usuarios, es aquél que haya instalado el DTI. En consecuencia, por ningún motivo los usuarios del SENASA, podrán instalar en los discos duros de las computadoras, ni utilizar por medio de Discos Compactos, llaves USB u otro medio, software no autorizado.
9. En caso de que los usuarios requieran instalar, ejecutar, o copiar de Internet programas (software) diferentes al instalado en sus equipos, deberán coordinar previamente con el DTI. Lo anterior, con el fin de evitar riesgos legales o de funcionamiento de los equipos.

9. Políticas relativas a la seguridad

9.1. Políticas generales de seguridad de acceso

1. El Departamento de TI es la responsable de la seguridad de acceso a los sistemas operativos, sistemas de información, bases de datos, y redes que operen en los equipos de cómputo del SENASA.
2. El Departamento de TI establecerá los mecanismos adecuados para el control, verificación y monitoreo de cambios en passwords, número de sesiones activas, seguridad lógica, física de todas las actividades relacionadas con el uso de tecnologías de información.
3. Para evitar situaciones de peligro para el SENASA, se desactivarán o bloquearán las cuentas de usuario a aquellas personas que estén en vacaciones, con permisos o incapacidades mayores a un mes, para lo cual debe informar la jefatura respectiva.
4. En caso de despido de un funcionario, el permiso de acceso deberá desactivarse o bloquearse previamente a la notificación de la persona sobre la situación. El Departamento de Recursos Humanos deberá notificar al Departamento de TI cuando se deba crear, cerrar o inhabilitar los accesos a un funcionario.
5. El administrador de los sistemas operativos, sistemas de información, bases de datos o redes asignará la clave de acceso al usuario.
6. Las Jefaturas que esté a cargo de la dependencia es responsable de notificar por escrito a la Dirección del Departamento de TI sobre el ingreso, salida o traslado de un usuario a su cargo. Esto con el fin de que se creen, inhabiliten, modifiquen o eliminen los privilegios de acceso a las diferentes plataformas, dominios y dispositivos correspondientes.

7. El encargado de seguridad informática no cambiará ninguna clave de acceso, si no es por solicitud expresa de su dueño. En caso de ser necesario y a solicitud de la jefatura se bloqueara los accesos de un usuario específico.
8. Salvaguardar la confidencialidad de la clave de acceso (password) y abstenerse de facilitarla a terceros por cualquier motivo. Cada usuario será responsable de las acciones que se reporten ejecutadas con clave de acceso. En los casos de sustitución, se asignará al sustituto, un nombre de usuario y una clave de acceso transitoria y nunca la correspondiente a la persona sustituida.
9. Cada usuario generará sus propias claves de acceso, cada cierto período de tiempo en la medida que las posibilidades técnicas que así lo permitan. Las conformará mediante el empleo de letras mayúsculas, minúsculas y números. El período lo establecerá el Departamento de TI, dependiendo de la sensibilidad de la información.
10. El usuario no debe dejar las claves de acceso escritas en medios o lugares donde puedan ser obtenidas por terceros (Ej.: monitor, carpetas, escritorio)
11. Cuando el usuario olvide u extravié su clave de acceso, deberá acudir al Departamento de Tecnología de Información e identificarse como propietario de la cuenta para que se le proporcione una nueva, o la utilización de cualquier otro medio de verificación que el Departamento de TI defina para la restauración de contraseñas.
12. La clave de acceso nunca debe ser compartida o revelada; hacer esto responsabiliza al usuario que presto su clave de acceso todas las acciones que se realicen con la misma.
13. El Departamento de Tecnología de Información implementara estrategias para que se generen clases de acceso con niveles adecuados de seguridad.
14. Los usuarios deberán aplicar medidas preventivas cuando se ausentan de las labores, antes de retirarse del lugar de trabajo donde se ubique el equipo de cómputo, el usuario deberá tomar las siguientes precauciones mínimas:
    a) Concluir las sesiones activas de cualquier sistema informático al finalizar las tareas;
    b) Proteger el equipo contra usos no autorizados mediante un mecanismo de bloqueo de seguridad autorizado por la Institución;
    c) Cerrar la conexión con los servidores.
15. Bajo ninguna circunstancia deberá compartirse la cuenta de usuario de Dominio o de Computadora asignada por el SENASA, ni la clave de acceso a dicha cuenta. Estas deberán manejarse conforme lo establezca la normativa interna del SENASA y el usuario a quien se le asigne será el único responsable del uso que les dé.
16. Está prohibido el almacenamiento, la transmisión, transferencia y, difusión de datos de carácter personal en los equipos del SENASA, sin contar con autorización válidamente emitida por quien esté legitimado para ello.
17. Los activos y recursos informáticos no deben conectarse a sistemas de cómputo ajenos al SENASA, a menos que sea estrictamente necesario para el cumplimiento de sus fines, en cuyo caso deben darse las siguientes condiciones:
    a) Que se sigan los procedimientos de seguridad adecuados para proteger la información propiedad del SENASA o que esté bajo su custodia.
    b) Que la conexión sea autorizada por el Departamento de TI.

18. En el caso de los funcionarios a quienes se les otorgue permiso con o sin goce de salario o para aquellos que concluyen su relación laboral con la institución, la Unidad de Recursos Humanos de la Dirección Administrativa Financiera, de inmediato pondrá esta situación en conocimiento del Departamento de TI, con el fin de que las correspondientes cuentas de correo, nombre de usuario y clave de acceso, sean temporalmente suspendidas o eliminadas, según corresponda.
19.

9.2. Políticas de seguridad de acceso a sistemas operativos

1. La activación y desactivación de usuarios de sistemas operativos estará a cargo del personal técnico del Departamento de TI.
2. En la activación de usuarios de sistemas operativos, se crearán identificadores de usuario utilizando el estándar de la letra inicial del nombre seguida del primer apellido.
3. Siempre que los sistemas operativos utilizados lo permitan, deberá controlarse el número de intentos de ingreso fallidos. Luego de 8 intentos, deberá bloquearse la cuenta del usuario y no permitir su ingreso al sistema. La cuenta debe estar bloqueada por 30 minutos y el administrador de seguridad podría desbloquearla antes por solicitud del usuario involucrado.
4. En el caso que el sistema operativo lo permita, se deberán implementar las bitácoras de seguimiento a los accesos, donde se registren los ingresos al sistema y los intentos fallidos.

9.3. Políticas de seguridad de acceso a sistemas de información

1. La activación y desactivación de usuarios de los sistemas de información estará a cargo del personal técnico del Departamento de TI.
2. El administrador del sistema de información asignará la clave de acceso al usuario.
3. Para otorgarle acceso a las diferentes aplicaciones del sistema, de acuerdo con las funciones que debe desempeñar el usuario, la jefatura correspondiente deberá hacer la solicitud formal al encargado de seguridad.
4. En toda transacción que se realice en el sistema se deberá grabar el nombre del usuario, la fecha y la hora en que se realizó.

9.4. Políticas de seguridad de acceso a bases de datos

1. El Departamento de TI velará porque toda base de datos que sea instalada, cuente con los controles de seguridad que garanticen la confiabilidad de la información.
2. Los códigos de acceso de los usuarios de las bases de datos utilizarán el estándar indicado en el respectivo de base de datos.

3. El administrador de la base de datos asignará la clave de acceso al usuario.
4. 4. El sistema de seguridad deberá contemplar el bloqueo de claves luego de tres intentos fallidos de acceso, cuando la base de datos lo permita.
5. El Departamento de TI implementará controles para que todos los respaldos de información, se encuentren almacenados en medios externos como cintas de respaldo, CD´s o DVD´s.
6. Los diferentes centros de datos del SENASA se respaldarán mutuamente en sus servidores y los medios físicos se resguardarán en los diferentes sitios.

9.5. Políticas de seguridad de acceso a redes

1. El administrador de redes asignará las claves de acceso a los usuarios, además procederá conforme con la activación y desactivación de usuarios de las redes del SENASA.
2. Para la utilización de las redes de datos, los nombres de usuario para las mismas se crearán siguiendo el esquema de letra inicial del nombre seguido por el primer apellido.
3. Para otorgarle acceso a las redes de datos, de acuerdo con las funciones que debe desempeñar el usuario, la jefatura correspondiente deberá enviar la solicitud formal al Departamento de TI.

9.6. Políticas de ubicación de los centros de procesamiento de información y comunicaciones

1. Los centros de procesamiento de información y comunicaciones deberán estar ubicados dentro del edificio del SENASA, a menos que se disponga instalarlos en sitios externos especializados con la seguridad necesaria.
2. Los centros de Datos deben estar completamente cerrados y con una única puerta de acceso, la cual deberá permanecer siempre cerrada. Las llaves de acceso estarán en custodia del personal del Departamento de TI.
3. Todo el cableado eléctrico que sea utilizado en los equipos de los centros de procesamiento de información y comunicaciones deberá ser totalmente independiente al cableado normal del edificio.
4. Para efectos de cableado eléctrico y de datos se utilizarán las normas de cableado que se fundamenten en las mejores prácticas utilizadas en el mercado.

9.7. Políticas de ambiente de los centros de procesamiento de información y comunicaciones

1. El área asignada para los centros de procesamiento de información y comunicaciones debe estar dotada con las condiciones ambientales necesarias para garantizar un entorno físico conveniente para su funcionamiento.
2. Este espacio de los centros de procesamiento de información y comunicaciones deberá estar climatizado permanentemente a una temperatura que se encuentre entre los 18º y 20º para garantizar el mejor rendimiento de los componentes electrónicos y alargar la vida útil de los mismos.

9.8. Políticas sobre "Responsabilidad de funcionarios por uso de los equipos"

1. Los funcionarios del SENASA usarán el equipo de cómputo en labores exclusivamente de trabajo y serán responsables por el uso adecuado de las herramientas tecnológicas.
2. Los usuarios deberán abstenerse de utilizar los recursos informáticos de la institución para realizar actividades personales o con fines lucrativos. Los recursos asignados deberán ser utilizados únicamente para cumplir los objetivos organizacionales.
3. El usuario del equipo mantendrá el equipo en un estado razonable de limpieza, para lo cual gestionará con su jefatura directa, los aditamentos necesarios (líquidos, franela, etc.) para el mantenimiento del mismo.
4. No deberá consumir ni preparar alimentos en la mesa destinada para el computador, para evitar derrame de los mismos sobre los equipos, que pueden ocasionar trastornos en su operación.
5. El costo por la reparación o sustitución de los equipos de cómputo a raíz de los desperfectos causados por situaciones de descuido en su uso, lo asumirá el usuario responsable, sin perjuicio de las sanciones disciplinarias que correspondan, para lo cual se seguirá el respectivo procedimiento administrativo.
6. El usuario del equipo es responsable de acatar las disposiciones del Departamento de TI, en cuanto a los programas que puede tener su equipo. Es responsable directo si es detectado en su equipo, un software no autorizado, ilegal o "pirateado", por lo cual debe responder ante las autoridades del SENASA o quien corresponda.
7. Es prohibido a todos los funcionarios de cualquier nivel, utilizar el equipo de la oficina para bajar de internet: juegos, música, videos, fotos, "screensavers" y todo archivo que provenga de fuentes no confiables; así como todo tipo de material pornográfico, que atenta contra el trabajo o el honor de las personas.
8. Ningún usuario está autorizado para almacenar material pornográfico, u ofensivo en ningún medio de almacenamiento de las computadoras, dispositivos periféricos u otro dispositivo de almacenamiento, mucho menos propagarlo a otras personas.
9. Los funcionarios deben velar porque su equipo tenga protección contra fallas de energía eléctrica o reducciones de voltaje. Para ello, deben prevenir a las jefaturas para que intercedan ante el Departamento de TI solicitud para dotar de estos dispositivos de seguridad.

10. Los usuarios deben utilizar antivirus actualizados para revisar todo medio antes de ingresarlo al equipo, con el propósito de evitar que éste sea contagiado al igual que la red institucional. Si no tienen instalado los antivirus tienen la responsabilidad de notificarlo al Departamento de TI.
11. Los usuarios de equipos deben procurarse los conocimientos imprescindibles para el manejo de sus programas, así como realizar copias de seguridad de los datos que considere relevante, lo cual puede resultar verdaderamente importante cuando los discos duros colapsen por cualquier razón.
12. Todo usuario es responsable de mantener respaldos de la información de acuerdo a sus necesidades. En caso de las aplicaciones el responsable por los respaldos es el administrador de la red y si es del caso, el Administrador de la Base de Datos.
13. Por razones de seguridad se prohíbe el uso de mensajería instantánea, chat o similares a menos que se justifique el uso para lo cual debe solicitarse por la jefatura, manifestándose los cuidados y supervisión que ejercerá sobre su uso.
14. Está prohibido conectarse a Internet utilizando equipos diferentes a los que oficialmente se encuentren en servicio.
15. Las computadoras son propiedad de la institución y son asignadas a los funcionarios para que desarrollen sus funciones en la institución, por tanto para efectos del SENASA toda la información contenida en las mismas es de carácter público. En caso de requerirse por cualquier motivo acceder al equipo de un funcionario, este no podrá alegar que la institución está violando su privacidad, por cuanto toda la información almacenada en los equipos es propiedad del SENASA; por tanto la información almacenada en las computadoras nunca puede ser de carácter privado.

10.Políticas Relativas al Desarrollo de Software

10.1. Política general de desarrollo de sistemas

1. El Departamento de TI debe estudiar la justificación y evaluar la factibilidad para llevar la modificación del sistema o nuevo proyecto.
2. El Departamento de TI, debe homologar y fomentar la utilización de las herramientas de apoyo disponibles en la Institución para el desarrollo de sistemas, que mejor se adapten a la metodología aplicada y que cumpla con los requisitos mínimos exigibles por los controles institucionales.
3. El Departamento de TI es responsable de la homologación de cualquier nuevo producto software usado para proyectos de Tecnología de Información.

10.2. Política para la recepción de requerimientos.

1. Toda solicitud de modificación a las aplicaciones o sistemas existentes, así como nuevos desarrollos debe presentarse a través de la Solicitud de Cambios o nuevos requerimientos de sistemas.

2. Las solicitudes de cambios o nuevos requerimientos de sistemas deben ser formalmente firmados por el Jefe de la dependencia solicitante y contar con la aprobación del Departamento de Tecnología de Información, antes de realizar el análisis o cualquier diseño inicial.
3. Los nuevos proyectos o modificaciones autorizados deben adherirse a un procedimiento formal de iniciación del proyecto, cuando el impacto de los mismos lo amerite, ya sea por su importancia en la organización como lo es un sistema de misión crítica o bien, por el tiempo de desarrollo e implantación estimados (mayor a 6 meses).

10.3. Política para la asignación de Recursos Económicos, Humanos y Materiales a los proyectos.

1. Para aquellos proyectos que dependan de la contratación de servicios o adquisición de bienes Informáticos, la definición de los recursos económicos dependerá del proyecto en el cual se llevará a cabo la contratación, pudiendo ser recursos propios, donación o convenio, para lo cual se deberán cumplir los procedimientos y normatividad establecidos por la Institución.
2. El Departamento de TI serán responsables de asignar al personal requerido para cada nuevo proyecto estableciendo según los roles establecidos en el proyecto.

10.4. Política para el manejo de los estándares para el desarrollo y la documentación.

1. El Departamento de TI se apegaran a una metodología estándar para el análisis y desarrollo de sistemas donde se definan los aspectos más importantes del ciclo de vida de desarrollo de sistemas y tecnología de información de la institución.
2. Los estándares de Análisis y Desarrollo incluirán estándar general para toda la documentación generada, incluyendo toda la documentación técnica (análisis, diseño, documentación de los programas, manuales de usuario).
3. Los estándares deben incluir una guía para el nombrado de objetos en una base de datos y mejores prácticas en la codificación de procedimientos y sentencias de SQL, contenida en “las políticas y procedimientos para la administración de bases de datos”.
4. El Departamento de TI es responsable de dar a conocer y vigilar la correcta aplicación de la metodología estándar para el desarrollo de sistemas, por todas y cada una de las personas involucradas en el área de Desarrollo.

10.5. Política para la contratación y supervisión de personal externo.

1. En la contratación de servicios externos, el Departamento de TI debe asegurarse de:
   1.1. Se cumple cabal y fielmente con la ley de contratación administrativa y en el caso de financiamiento externo cumplir con la Normatividad Correspondiente.
   1.2. El contrato prevé los riesgos más frecuentes cuando se contratan servicios externos e incorpora las penalizaciones en caso de incumplimiento de contrato por parte del proveedor, en este caso El Departamento de TI trabajara de forma conjunta con el Departamento de Proveeduría.
   1.3. El personal externo que intervenga en los proyectos debe cumplir, al menos, los mismos requisitos que se exigen a los empleados del Departamento de TI.

1.4. El Departamento de TI debe supervisar el trabajo realizado, certificándolo antes del pago.
1.5. El trabajo o proyectos realizados por el proveedor, deben ser compatibles con los estándares establecidos por la Institución.

10.6. Política para el control de cambios en Desarrollo.

1. El Departamento de TI es el responsable de elaborar, difundir y vigilar la correcta aplicación del procedimiento de control de cambios.

10.7. Política para el Análisis de requerimientos.

1. Para todo requerimiento autorizado debe desarrollarse un análisis de requerimientos cuyo fin debe ser establecer las especificaciones formales que describan las necesidades de información que deben ser cubiertas por el nuevo sistema.
2. En la definición de los requerimientos deben participar los usuarios de todas las unidades a las que afecte el nuevo sistema o las modificaciones solicitadas.
3. Debe existir un antecedente (minuta de trabajo, correo electrónico) para cada una de las sesiones con los usuarios del proyecto y con los responsables de las unidades afectadas que permita conocer cómo valoran el sistema actual (en caso de que exista) y lo que esperan del nuevo sistema.
4. El plan revisado debe incluir para cada entrevista, la fecha, hora y lugar, tipo de entrevista (individual, en grupo, por escrito, etc.) y un apartado de los aspectos relevantes que en dicha entrevista se tratarán. (Funciones que el entrevistado realiza y los problemas que necesita resolver).
5. Una vez presentados los requisitos del nuevo sistema o la modificación solicitada, se deben definir las diferentes alternativas de construcción con sus ventajas e inconvenientes.
6. Para la selección de la alternativa se debe contar con un documento en el que se describen las distintas alternativas.

10.8. Política para el Diseño Lógico (Casos de Uso)

1. Para todo requerimiento autorizado debe desarrollarse un diseño lógico y técnico.
2. El Diseño Lógico deberá contemplar:
   1.6. Se debe documentar de manera completa e integral el Diseño lógico, respetando los estándares establecidos por el Departamento de TI.
   1.7. Debe contemplar la estructura modular del sistema.
   1.8. Debe existir un documento con el diseño de la estructura modular del sistema.
   1.9. Los módulos deben estar diseñados para poder ser usados adecuadamente por otras aplicaciones, en caso de ser necesario.
   1.10. Se debe validar que los componentes o programas del nuevo sistema se definieron.
   1.11. Debe definirse la forma en que el nuevo sistema interactúa con los distintos usuarios.

1.12. Se debe describir con detalle suficiente las pantallas a través de las cuales el usuario navegará por la aplicación, incluyendo todos los campos significativos, teclas de función disponibles, menús, botones, etc.

1.13. Se deben describir con detalle suficiente los informes o reportes que se obtendrán del sistema y los formularios asociados.

1.14. La especificación del nuevo sistema debe considerar los requisitos de seguridad, rendimiento, copias de seguridad, recuperación y depuración de datos.

1.15. Se debe analizar el nuevo sistema con el propósito de localizar sus interacciones y contactos con otros sistemas a fin de determinar si existe un sistema integral de información, sistemas aislados o simplemente programas.

1.16. Se deben considerar todas las necesidades de información de las áreas de negocios o usuarias.

1.17. Debe observar los estándares establecidos por la Subdirección de Administración de Datos (nomenclatura, validación de campos y archivos, etc.)

1.18. Debe existir un diccionario de datos que describa cada uno de los campos contenidos en las bases de datos existentes.

1.19. Se deben definir los tiempos de respuesta en el diseño para que estos sean iguales a los requeridos y que el ordenamiento de las bases de datos sea rápido y confiable.

1.20. El diseño lógico debe incluir el esquema de seguridad en donde se debe especificar un estricto control de acceso a través de la identificación y autenticación de los usuarios.

1.21. El diseño lógico debe incluir la asignación de privilegios de acceso de acuerdo a las funciones de los usuarios con base en la estrategia de “necesidad de acceder” necesidad de conocer, considerando adicionalmente los privilegios de adicionar, cambiar y borrar datos.

1.22. Dependiendo de la importancia estratégica de la aplicación, el modelo de seguridad lógica, deberá incluir una bitácora en donde se registren los accesos realizados y los cambios hechos a las bases de datos.

3. El Diseño Técnico deberá contemplar:

1.1. Se debe definir una arquitectura física para el sistema, que sea congruente con las especificaciones funcionales y con el entorno tecnológico elegido o con el existente.

1.2. El entorno tecnológico debe estar definido en forma clara y apegarse a los estándares existentes en el área de Tecnología de Información.

1.3. Se deben definir perfectamente todos los elementos que configuran el entorno tecnológico para el proyecto (servidores, ordenadores personales, periféricos, sistemas operativos, conexiones de red, protocolos de comunicación, sistemas gestores de bases de datos, compiladores, herramientas de apoyo, middleware, librerías, etc.).

1.4. Se debe validar la existencia de los elementos seleccionados dentro de los estándares de la Dirección de Ingeniería de Sistemas, también se debe medir la capacidad de respuesta a los requisitos establecidos de volúmenes, tiempos de respuesta, seguridad, etc.

10.9. Política para la construcción de Sistemas.

1. Se debe preparar adecuadamente el entorno de desarrollo y pruebas, así como los procedimientos de operación, antes de iniciar el desarrollo.
2. Se deben de considerar los siguientes puntos:
   1.5. Crear e inicializar las bases de datos o archivos necesarios que cumplan las especificaciones realizadas en el módulo la etapa de diseño.
   1.6. No se debe trabajar en ningún momento con información del ambiente de producción o explotación.
   1.7. Se debe validar que todos los elementos lógicos y físicos para la realización de los tipos de pruebas se encuentren disponibles.
   1.8. Se debe desarrollar todos los procedimientos de usuario apegándose a los estándares del Departamento de TI
   1.9. Se debe programar, probar y documentar cada uno de los componentes identificados en el diseño del sistema.

10.10. Políticas para el aseguramiento de la Calidad.

1. Debe existir un plan de pruebas de aceptación del sistema, el cual debe ser coherente con los requisitos, la especificación funcional del sistema y la infraestructura existente.
2. El plan de pruebas de aceptación, debe incluir todos los recursos necesarios (Humanos, Materiales así como de Hardware y Software).
3. Se deben realizar los siguientes tipos de pruebas:
   1.10. Pruebas unitarias (pruebas ejecutadas por el desarrollador del módulo del sistema o de la modificación requerida, su objetivo es validar la funcionalidad del módulo en forma aislada).
   1.11. Pruebas conjuntas (pruebas ejecutadas por todos los desarrolladores de cada uno de los módulos del sistema, su objetivo es validar la funcionalidad del sistema completo).
   1.12. Los usuarios involucrados deberán realizar pruebas de aceptación de los sistemas antes de su liberación al ambiente de producción.
   1.13. El Departamento de TI debe asegurar el cumplimiento de los estándares establecidos para todo el ciclo de vida de desarrollo del proyecto.

10.11. Política para la implantación del nuevo sistema desarrollado o la modificación realizada en el ambiente de producción.

1. Departamento de TI debe contemplar un plan de instalación del sistema o modificación a liberar en el ambiente de producción.
2. El plan de instalación del sistema debe ser definido desde las primeras etapas (análisis), con el fin de considerar todos los factores que influirán en la implantación. Esto evitará que surjan situaciones no previstas que afecten las fechas y calidad de la implantación. La anticipación de este plan ayudará a identificar necesidades de capacitación, depuración de información, conversión de datos, logística, etc.

3. Se debe validar que el sistema desarrollado o la modificación realizada, cumple con los requisitos establecidos en la fase de análisis.
    1.14. El sistema desarrollado o la modificación realizada, debe ser aceptado formalmente por los usuarios antes de ser liberado a producción.
    1.15. De aplicar, se deben realizar las pruebas del sistema que se especificaron en la fase de pruebas.
    1.16. El sistema desarrollado o la modificación realizada, se debe poner en producción formalmente y pasará a estar en mantenimiento sólo cuando haya sido aceptado y esté preparado todo el entorno en el que se ejecutará.
    1.17. Si existe un sistema anterior, el sistema nuevo se pondrá en producción de forma coordinada con la retirada del anterior, migrando los datos si es necesario.
    1.18. En caso de aplicar, debe haber un período de funcionamiento en paralelo de los dos sistemas (nuevo y anterior), hasta que el nuevo esté funcionando con todas las garantías. Sin exceder los tiempos en el paralelo definidos entre los usuarios y Sistemas.
    1.19. De aplicar, el sistema anterior sólo se debe usar en modo de consulta, únicamente para obtener información, sólo en el caso de que la información del sistema anterior no ha sido migrada al nuevo.
    1.20. Los usuarios responsables deberán firmar un acta de liberación del sistema a producción.
    1.21. Dependiendo de la naturaleza del proyecto se recomienda realizar un procedimiento para llevar a cabo el mantenimiento. Este debe estar aprobado por el Departamento de TI y los usuarios responsables.
    1.22. El procedimiento para realizar el mantenimiento debe tener en cuenta los tiempos de respuesta máximos que se pueden permitir ante situaciones de no funcionamiento.
4. Para reportar y dar seguimiento a cualquier problema o para el mantenimiento del sistema debe aplicarse el procedimiento de establecido por el Departamento de TI para estos efectos.
5. Es responsabilidad del Departamento de TI asegurarse de que sus colaboradores conozcan y apliquen las políticas y procedimientos de desarrollo de sistemas.

11.Políticas relativas al cumplimiento de las normas

1. Todo usuario que reciba y tenga bajo su custodia bienes del Estado, será responsable por el uso adecuado y el cuidado del equipo de cómputo asignado. Cualquier daño, pérdida, abuso o empleo ilegal que le sea imputable por falta al deber de cuidado, negligencia o dolo será responsabilidad del usuario principal y de las Jefaturas o encargados cuando se compruebe negligencia de su parte en su deber de control de los recursos informáticos asignados en sus dependencias.

2. Para la sana administración de sus sistemas informáticos y a fin de evitar y controlar instrucciones maliciosas, personal autorizado del Departamento de TI procederá, a llevar a cabo revisiones periódicas en sus sistemas y equipos de cómputo, a fin de garantizar que se encuentran libres de códigos malignos, así como asegurar que los usuarios posean instalado el software estándar y/o aprobado por el SENASA. Esta actividad siempre se realizara en presencia del usuario encargado del equipo.
3. La jefatura o encargado de cada dependencia será el responsable de velar por que estas disposiciones se cumplan y reportará a la mayor brevedad al Departamento de TI cualquier anomalía que se presente. Asimismo, la Jefatura podrá también solicitar al Departamento de TI una revisión técnica del sistema informático en aquellas dependencias donde existan indicios de una utilización inadecuada de éstos.
4. El Departamento de TI del SENASA, por medio de sus diferentes áreas u Unidades será el ente contralor de la administración de los recursos informáticos en el SENASA.
5. Las faltas cometidas al tenor de lo dispuesto en el presente documento, serán sancionadas de conformidad con las disposiciones establecidas en el Código de Trabajo y el Reglamento Autónomo de Servicios de la Institución, así como las demás disposiciones vigentes y aplicables, sin perjuicio de las responsabilidades civiles y penales que deba asumir el infractor.

Glosario de términos utilizados

A continuación se presentan en orden alfabético una serie de términos que son utilizados en el presente reglamento:

- Área de Tecnologías de Información: lugar físico específico donde se encuentra equipo de cómputo especializado.
- Base de Datos: Conjunto de datos organizados de tal modo que permita obtener con rapidez diversos tipos de información.
- Browser: Programa o aplicación informática que se usa para navegar por las redes informáticas y acceder a documentos, imágenes y demás información.
- CD: Siglas en inglés de Disco Compacto (Compact Disk), placa circular de material plástico donde se graba información por medio de láser codificado.
- Chat: Conversación interactiva en tiempo real, en Internet.
- Cookies: Archivo que se implanta en el disco duro del usuario por el sitio visitado en Internet, contiene información acerca del usuario.
- Correo Spam: Se utiliza este término para identificar todo aquel correo denominado como “Correo Basura” o correo no deseado.

- Hardware: junto de componentes que integran la parte material de una computadora, impresora o equipo de comunicación.
- Internet: Red informática de comunicación internacional que permite el intercambio de todo tipo de información entre sus usuarios. El nombre proviene del acrónimo de las palabras inglesas International Network (red internacional).
- Normativa: Conjunto de normas aplicables a una determinada materia o actividad.
- Outsourcing: termino en idioma ingles para La subcontratación, externalización o tercerización
- Perfil de usuario: Grupo de privilegios o roles de trabajo que se asignan a una persona, de acuerdo con las características que tenga su puesto con el fin de que pueda desempeñar sus funciones.
- Rol: Grupo de derechos o privilegios para el uso de recursos informáticos que asignan a uno o más usuarios, por ejemplo: derechos de lectura, escritura, modificación o borrado sobre una tabla de datos.
- Recuperación: Es la tarea que se lleva a cabo cuando es necesario volver al estado de la aplicación al momento del último respaldo, a partir de los datos de la última copia de seguridad realizada.
- Respaldo: Es la obtención de una copia de los datos en otro medio magnético, de tal modo que a partir de dicha copia es posible restaurar el sistema o la información.
- Seguridad lógica: Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.
- SENASA: Servicio Nacional de Salud Animal
- Software: Es un término genérico que designa al conjunto de programas de distinto tipo (sistema operativo y aplicaciones diversas) que hacen posible el funcionamiento y la operación del computador.
- TI: Tecnología de Información.
- Virus: Es un programa informático que se ejecuta en el ordenador sin previo aviso y que puede corromper el resto de los programas, archivos de datos e incluso el mismo sistema operativo.
-